TASK ORDER

GSQ0015AJ0071

Technical Assurance Support

in support of:

United States Cyber Command (USCYBERCOM)

Issued to:
CACI, Inc.
GSA Alliant

Issued by:
The Federal Systems Integration and Management Center (FEDSIM)
1800 F Street, NW
Suite 3100 (QF0B)
Washington, D.C. 20405

September 2015

FEDSIM Project Number AF00756

SECTION C –STATEMENT OF WORK

C.1 BACKGROUND

The United States Cyber Command (USCYBERCOM) was established 31 October 2010 with the merging of Joint Task Force-Global Network Operations (JTF-GNO) and Joint Functional Component Command-Network Warfare (JFCC-NW). This requirement supports USCYBERCOM and Cyber Mission Force (CMF). The CMF is comprised of three command forces (Cyber National Mission Force (CNMF), Cyber Combat Mission Force, and Cyber Protection Force) that were created to help defend and react to a cyber-attack on the nation. USCYBERCOM works closely with the Office of the Under Secretary of Defense for Intelligence (OUSD(I)) to maintain the Department of Defense Technical Assurance Standard (TAS) for Computer Network Attack (CNA) Capabilities.

United States Strategic Command (USSTRATCOM), to which USCYBERCOM is a sub-unified command subordinate, is responsible for the global command and control of U.S. strategic forces to meet decisive national security objectives by deterrence and defense against enemy attack. USSTRATCOM provides a broad range of strategic capabilities and options for the President and Secretary of Defense, and specialized expertise to the joint warfighter. It is the command and control center for U.S. strategic forces and controls military space operations, computer network operations, information operations, strategic warning and intelligence assessments as well as global strategic planning. It ensures that forces of hostile nations cannot prevent U. S. use of space, while enhancing the space operations of U.S. and Allied forces. Additionally, USSTRATCOM has responsibility for Information Assurance (IA) for all U.S. military agencies.

USCYBERCOM's mission areas include full-spectrum global strike, space operations, computer network operations, Department of Defense (DoD) information operations, strategic warning, integrated missile defense, global Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR), nuclear deterrence, and deterence and defense against the proliferation of weapons of mass destruction (WMD). USCYBERCOM is charged with unifying existing cyberspace resources, creating synergy that does not currently exist and synchronizing war-fighting effects to defend the information security environment.

USCYBERCOM's organizational structure consists of multiple Joint Directorates that each have an individual mission and purpose that relates to the overall USCYBERCOM mission. This requirement addresses the support needed by three specific Joint Directorates, Joint Directorate 6 (J6), that is responsible for systems and Chief Information Officer (CIO) support; Joint Directorate 8 (J8), that is responsible capability and resource integration; and Joint Directorate 9 (J9), that oversees advanced concepts and technology.

C.1.1 PURPOSE

The purpose of this Task Order (TO) is to provide Technical Assurance (TA) Information Technology (IT) and Research, Development, Test and Evaluation (RDT&E) support to the USCYBERCOM.TA is defined as the basis for confidence that CNA capabilities will meet its technical objectives including the tools and techniques used to develop, analyze, and implement a capability. USCYBERCOM, in coordination with key stakeholders (and in part through the use of this TO) will deter and defeat adversary attacks in cyberspace to defend U.S. national interests and ensure U.S. freedom of action in and through cyberspace, and deny the same to adversaries.

C.1.2 AGENCY MISSION

J6 is responsible for providing premier Command, Control, Communications, Computers and Information Technology (C4IT) capabilities for USCYBERCOM to conduct full-spectrum military cyberspace operations. In addition, J6 shapes the cyberspace domain in support of USCYBERCOM's lines of operations through enhanced command and control and enterprise architectures and risk management strategies.

J8 oversees the business operations and resource management and provides contract management performing all acquisition support planning, and responsible for travel management. Additionally, J8 manages the planning, programming, and budget process and performs all funds control functions associated with the authorization of use and commitment of Government funds.

J9 drives delivery of tactics, techniques, and procedures (TTPs) and corresponding material capability solutions designed to meet USCYBERCOM and Combatant Command (CCs) cyberspace requirements across full spectrum cyberspace operations.

C.2 SCOPE

The scope of this requirement focuses primarily on providing TA support services to USCYBERCOM. In support of this requirement the contractor shall research, develop, demonstrate, integrate, and test innovative technologies that defend against cyberspace threats and support network management. The contractor shall also develop techniques that provide a means to leverage expertise and applications from alternative cyber intelligence assessment perspectives and merge them to provide a situational awareness (SA) perspective to DoD Combatant Commands/Services/Agencies/Field Activities (CC/S/A/FAs). The contractor shall provide USCYBERCOM with high quality, efficient and effective, performance-based engineering services in the areas of research, development, test and evaluation. To ensure effective and efficient operations for the full scope of USCYBERCOM TA responsibilities, support shall be required in the following areas:

a. Provide Program Management
b. Provide TA Support
c. Provide TA Training
d. Research, Develop, Analyze, And Test Cyber Related Capabilities
e. Provide Capability and Resource Integration Support
f. Provide Program and Technical Support
g. Provide Technical Assistance
h. Provide IA, Configuration Management (CM) and Technical Writing Support

The Government requires the contractor to ensure that all enumerated tasks are completed and recognizes that the contractor's scope of work will vary between the different identified Joint Directorates. Each identified task in Section C.5, Tasks, will identify the Joint Directorate to which that task is aligned. Task 1 – Provide Program Management is not Joint Directorate specific.

The contractor shall perform primarily at Fort George G. Meade, Maryland; however some long-distance travel may be required to support cyber exercises. Additionally, for contingencies and

Continuity of Operations (COOP), the contractor may be required to provide support from an alternate place of performance if required by the Government.

Personnel may be required to travel to contiguous U.S. (CONUS) or outside the contiguous U.S (OCONUS) locations for work-related conferences, meetings, training or exercises. Typically, contractor personnel will accompany Government personnel on travel for no more than seven calendar days per occurrence. All travel shall be approved by the Contracting Officer Representative (COR) prior to occurrence.

The Transition-out period is 120 days to allow for the time necessary to activate security clearances and provide any follow on contract adequate time to transition-in.

C.3 CURRENT INFORMATION TECHNOLOGY (IT)/NETWORK ENVIRONMENT

Technical support shall be primarily provided in two environments, the TA evaluation environments and the individual lab environments that support research and development of cyber capabilities. Details on the type of technical support required are specified in Section C.5.7, Task 7 – Provide Technical Assistance.

C.4 OBJECTIVE

In order to maintain dominance in the cyber realm, USCYBERCOM's requires highly skilled personnel who will combat threats to U.S. and Allied interests on a global scale.

C.5 TASKS

C.5.1 TASK 1 – PROVIDE PROGRAM MANAGEMENT

The contractor shall provide program management support under this TO. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this Statement of Work (SOW). The contractor shall identify a Program Manager (PM) by name who shall provide management, direction, administration, quality assurance, and leadership of the execution of this TO.

C.5.1.1 SUBTASK 1 – COORDINATE A PROJECT KICK-OFF MEETING

The contractor shall schedule, coordinate, and host a **Project Kick-Off Meeting (Section F, Deliverable 01)** at the location approved by the Government. The meeting will provide an introduction between the contractor personnel and Government personnel who will be involved with the TO. The meeting will provide the opportunity to discuss technical, management, and security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include Key contractor Personnel, representatives from the Directorates, other relevant Government personnel, and the COR.

C.5.1.2 SUBTASK 2 – PREPARE A MONTHLY STATUS REPORT (MSR)

The contractor shall develop and provide an **MSR (Section F, Deliverable 02)** in accordance with **Section J, Attachment B** using Microsoft (MS) Office Suite applications, by the tenth of each month via electronic mail to the Technical Point of Contact (TPOC) and the COR. The MSR shall include, but not limited to the following:

a. Activities during reporting period, by task (include: on-going activities, new activities, activities completed; progress to date on all above mentioned activities). Start each section with a brief description of the task.
b. Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.
c. Identified risk and mitigations.
d. Personnel gains, losses, and status (security clearance, etc.). The contractor shall provide an up-to-date matrix mapping of all personnel to tasks.
e. Government actions required.
f. Schedule (show major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
g. Summary of trips taken, conferences attended, etc. (attach Trip Reports to the MSR for reporting period).
h. Accumulated invoiced cost for each CLIN up to the previous month.
i. Projected cost of each CLIN for the current month.

C.5.1.3 SUBTASK 3 – CONVENE MONTHLY STATUS MEETINGS

The contractor's PM shall convene a Monthly Status Meeting with the TPOC, COR, and other Government stakeholders. The purpose of this meeting is to ensure all stakeholders are informed of the monthly activities, opportunities are provided to identify other activities and establish priorities, and problem or opportunity resolution is coordinated. The contractor PM shall provide **Monthly Status Meeting Minutes (Section F, Deliverable 03)** of these meetings, including attendance, issues discussed, decisions made, and action items assigned, to the COR within five workdays following the meeting.

C.5.1.4 SUBTASK 4 – CONDUCT QUARTERLY MANGEMENT REVIEWS AND BRIEFINGS

The contractor shall conduct a Quarterly Management Review of progress and provide a **Quarterly Briefing (Section F, Deliverable 04)** on the program status. The Quarterly Management Briefing shall include a summary of the major points from the written MSR.

C.5.1.5 SUBTASK 5 – PREPARE PRESENTATION MATERIALS/BRIEFING MATERIALS/MINUTES

The contractor shall provide copies of the following for conferences and meetings:

a. Presentation Material **(Section F, Deliverable 05)** shall be provided for Government approval at least five working days before distribution or presentation, unless otherwise specified. The contractor shall provide the Government with copies for review to include at a minimum a soft copy format and readable through Command standard format(s).

b. Conference Minutes **(Section F, Deliverable 06)** that document contractor participation at conferences and meetings in support of the TO.

C.5.1.6 SUBTASK 6 – PREPARE A PROJECT MANAGEMENT PLAN (PMP)

The contractor shall prepare and deliver a **Draft and Final PMP (Section F, Deliverables 07 and 08).**

The PMP shall contain at a minimum the following:

a. Describe the proposed management approach.
b. Include milestones, deliverable schedule, tasks, and subtasks required in this Contract.
c. Provide an overall Work Breakdown Structure (WBS) and associated responsibilities and partnerships between Government organizations.
d. Quality management
e. Staffing management
f. Logistics management
g. Training approach.

C.5.1.7 SUBTASK 7 – PREPARE TRIP REPORTS

The Government will identify the need for a Trip Report (if required) when a request for travel is submitted. The contractor shall submit Trip Reports five working days after completion of a trip for all long distance travel **(Section F, Deliverable 22).**

The Trip Report shall include the following information:

a. Personnel traveled
b. Dates of travel
c. Destination(s)
d. Purpose of trip
e. Cost of the trip
f. Approval authority
g. Summary of events, action items and deliverables

The contractor shall keep a summary of all long-distance travel including, but not limited to, the name of the employee, location of travel, duration of trip, and point of contact (POC) at travel location.

C.5.1.8 SUBTASK 8 - QUALITY CONTROL PLAN (QCP)

The contractor shall provide a **Quality Control Plan (QCP) (Section F, Deliverable 09**) that details and describes the contractor's framework and processes for delivering quality products and services required by the tasks in this TO. The contractor shall ensure that the services are performed in accordance with commonly accepted commercial practices. The contractor shall develop quality control procedures that address the Task Area services in the TO. The contractor shall provide the requisite staffing and procedures to meet the quality, quantity, timeliness, responsiveness, customer satisfaction, and service delivery and performance requirements of this effort. The contractor shall identify the applicable processes and metrics used to self-assess

performance, in addition to the resources to be applied to this effort. The contractor's QCP shall be submitted to the Government within 30 days of TO Award (TOA). The Government will evaluate the contractor's performance by appointing a Quality Assurance Personnel (COR/TPOC), to monitor performance to ensure services are received. The COR will evaluate the contractor's performance through intermittent inspections of the contractor's quality control program and receipt of complaints from base personnel.

C.5.1.9 SUBTASK 9 – FACILITATE TRANSITION-OUT

The Transition-Out Plan shall facilitate the accomplishment of a seamless transition from the incumbent to an incoming contractor/Government personnel at the expiration of the TO. The contractor shall provide a **Transition-Out Plan (Section F, Deliverable 10)** within 180 calendar days of TOA. The Transition-Out period is expected to last 120 calendar days. The contractor at a minimum shall identify how it will coordinate with the incoming contractor and/or Government personnel to transfer knowledge regarding the following:

a. Project management processes
b. Points of contact
c. Location of technical and project management documentation
d. Status of ongoing technical initiatives
e. Appropriate contractor-to-contractor coordination to ensure a seamless transition
f. Transition of Key Personnel
g. Schedules and milestones
h. Actions required of the Government
i. Government Furnished Property (GFP) inventory.

The contractor shall also establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings.

C.5.1.10 SUBTASK 10 – IMPLEMENT TO TRANSITION-OUT

The contractor shall implement its Transition-Out Plan no later than (NLT) 120 calendar days prior to expiration of the TO.

C.5.2 TASK 2 – PROVIDE TECHNICAL ASSURANCE (TA) SUPPORT (J9)

The contractor shall support USCYBERCOM's J9 Directorate in providing TA. USCYBERCOM's J9 Directorate provides TA services to DoD community by ensuring that the technical integrity of developed cyber tools, systems, and capabilities are in accordance with approved TA policy documents. USCYBERCOM has developed TA policy documents, which are tailored from the overarching DoD TA policy document, and provide specialized guidance to the DoD community. The TA policy documents establish TAS (as documented in TA policy documents) that provide guidance on the process and procedure to ensure developed cyber tools, systems, and capabilities are properly tested before deployment.

USCYBERCOM's role within the DoD continues to expand as an oversight body for TA of cyber related tools, systems, and cyber capabilities. Accordingly, support for this task is anticipated to become increasingly more visible and mission critical.

C.5.2.1 SUBTASK 1 – ASSIST WITH TECHNICAL ASSURANCE OVERSIGHT (J9)

The contractor shall provide support to established DoD oversight body(s) by organizing meetings, preparing **TA Oversight Minutes (Section F, Deliverable 11)**, and maintaining updates to the TA policy documents. The contractor shall organize and contribute to any TA conferences/workshops that may be scheduled. The contactor shall provide support for the development of technical oversight to all TA laboratories supporting the DoD and prepare TA validation reports to provide guidance and direction to the TA laboratories on the proper implementation of the TAS. The contractor shall provide interpretation and guidance of TA policy documentation that supports the in progress lab accreditation program, which ensures laboratories can operate according to established guidelines. The contractor shall monitor and review TA evaluation results by examining evaluation reports, as defined in Section C.5.2.2.

The contractor shall develop and maintain documentation of **TA Standards (Section F, Deliverable 12)** that are included within the TA policy documents. . The contractor shall research and respond to queries regarding interpretation of the TA policy documents and as it applies to USCYBERCOM.

The contractor shall conduct peer reviews of new implementation documentation and facilitate meetings to manage and approve changes to the USCYBERCOM TAS.

C.5.2.2 SUBTASK 2 – CONDUCT TECHNICAL ASSURANCE EVALUATIONS AND OPERATIONAL ASSESSMENTS (J9)

The contractor shall complete TA evaluations in accordance with TA policy documents DoD Instruction O-3600.03, Technical Assurance Standards for Computer Network Attack (CNA) Capabilities, 22 April 2010. TA evaluations are conducted on developed cyber tools, systems, and capabilities in a test environment to ensure that technical integrity is in accordance with approved TA policy documents. The Government estimates that there are approximately five TA evaluations required per year with the possibility for additional TA evaluations as the USCYBERCOM mission requirements expand and evolve to new cyber threats.

The contractor shall complete operational assessments of cyber tools, systems, and capabilities in support of USCYBERCOM's mission. Operational assessments are conducted after TA evaluations are completed and occur in an operational environment on cyber tools, systems, and capabilities. The contractor shall also support the collection of intelligence in support of operations. The contractor shall support other services and the Intelligence Community (IC) TA evaluations and operational assessment teams. TA evaluation teams will typically support the operational assessments of the cyber tool, system, or capability being implemented.

The contractor shall assist other TA and operational assessment teams by providing direct participation, consulting, monitoring and training. The contractor shall schedule the resourcing of evaluators to ensure that the requirements of each TA evaluation are met.

The contractor shall perform and support TA evaluations and operational assessments in support of the USCYBERCOM mission. This support shall include, but is not limited to the following:

a. Develop **Test and Evaluation Plans (Section F, Deliverable 13)** that include test procedures and corresponding rating results for cyber tools, systems, and capabilities.
b. Conduct testing in accordance with approved Test and Evaluation plans to ensure proper operation of cyber tools, systems, and capabilities throughout the entire life cycle.

c. Plan and develop test environments to be integrated into the USCYBERCOM test enterprise architecture.

d. Conduct prototype assessments in field environments, operate test instrumentation, and support remote testing.

e. Compile and analyze documentation, data, and other products to evaluate and validate sensor system performance capabilities and effectiveness, assess risk, and determine operational feasibility and benefits of USCYBERCOM systems or technology prototypes to include recommending assessments of system performance, identifying deficiencies, and investigating physical science phenomena.

f. Assist with leading wargame efforts and coordinate with functional area experts including operational cyber subject matter experts, senior policy subject matter experts, Modeling and Simulation (M&S) development experts; and provide administrative and logistics support, as needed, for facilitation with wargame seminars and capstone events.

g. Conduct evaluations of the quality of proposed and existing software systems and solutions that support various cyber software activities to be integrated into various networks and architectures.

h. Analyze capabilities for potential vulnerabilities that may result from improper system configuration, hardware or software flaws, or operational weaknesses.

i. Present any security issues that are found, to the system owner, with an assessment of their impact and a recommendation for mitigation, or a technical solution.

j. Assess system information security policies against approved policy documentation.

k. Ensure policies are comprehensive to the system.

l. Review technical reports.

m. Evaluate capabilities components against their ability to resist threats in the deployed environment, configurations, and implementation of firewalls, proxy servers, routers, Virtual Private Networks (VPNs), Intrusion Detection Systems (IDS), wireless networks, etc., against legal requirements and departmental /local procedures associated with operations.

n. Conduct penetration testing projects, including:

    1. Internal Penetration Testing (Networks, Servers, Workstations), stealth techniques for evading Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) web services, remote access, etc..
    2. Web application penetration testing (anonymous and authenticated).
    3. Data exfiltration assessments (i.e. the unauthorized transfer of sensitive information from a target's network to a location which a threat actor controls).

o. Perform tests and experimentation in support of USCYBERCOM test activities to include test architecture development, equipment calibrations, repairs, modifications, and adjustments to support task objectives.

p. Conduct capability vulnerability assessments and testing, customized to the system function and technical requirements, and based on status within security assessment and authorization cycle and authority to operate status.

C.5.3 TASK 3 – PROVIDE TECHNICAL ASSURANCE TRAINING (J9)

The contractor shall assist USCYBERCOM's J9 Directorate in ensuring that TAS, as detailed in TA policy documents, are adhered to for all DoD Government personnel that are identified as having to follow the set guidance. J9 conducts regular training to meet this objective.

C.5.3.1 SUBTASK 1 – DEVELOP TECHNICAL ASSURANCE TRAINING (J9)

The contractor shall develop, maintain, and periodically publish **TA Training Materials (Section F, Deliverable 14),** to include at a minimum the following:

a. Training plans
b. Course catalogs
c. Training schedules
d. Procedural documents that may be required
e. Develop and update TA classes including any associated training aids, exercises, and tests.

C.5.3.2 SUBTASK 2 – CONDUCT TECHNICAL ASSURANCE TRAINING (J9)

The contractor shall teach TA classes. The contractor shall perform all logistical activities required for course instruction to include the following:

a. Securing classroom locations
b. Preparing/disseminating course announcements,
c. Registering students
d. Preparing instructional materials and classrooms
e. Coordinating with Subject Matter Experts (SMEs)
f. Preparing certificates

The contractor shall maintain training records in a currently deployed Government database that can easily be manipulated to gather the tailored statistics required by the Government.

Each TA training course shall be piloted to obtain feedback and updated as necessary to include modifications to the class format, duration, and content.

The contractor shall maintain the internal TA Evaluator Development Training Program, which determines evaluator training requirements and how they will be met. The contractor shall maintain records that facilitate determining each evaluator's developmental progression.

Training is held in a classroom at Fort George G. Meade. Classes vary in length from one to five days and range from five to ten attendees. TA Training classes are anticipated monthly.

C.5.4 TASK 4 – RESEARCH, DEVELOP, ANALYZE, AND TEST CYBER RELATED CAPABILITIES (J9)

The contractor shall support J9 in conducting research on new advanced cyber technologies and emerging cyber capabilities, in conjunction with outside DoD agencies and academia, to support

the mission of CMF and USCYBERCOM. This task captures the research and development, and the subsequent analysis and testing of this evolving IT field.

The support for new advanced cyber technologies and emerging cyber capabilities can vary in size, scope, and complexity. The ability to definitively define all support to the objective of this task is not possible due to nature of the research and developments aspects of the work. The Government anticipates that the support shall include, but is not limited to, the following:

a. Evaluate and document cyber security tools in support of the Mission Forces Tools Project, which has an estimated completion date of the end of the first quarter of Fiscal Year (FY) 2016. This critical project supports the CMF in the identification and evaluation of cyber-specific tools that will assist in the defense and reaction to cyber attacks on U.S. and Allied IT assets.

b. Completion of the Rapid Tool development project by the second quarter of FY 2016. This development project involves the evaluation, configuration, and alignment of a suite of Rapid Application Development (RAD) cyber security tools that are critical to maintaining and improving the Mission Forces cyber posture. Rapid is a tool that is used to ingest other tools and identify their core components thereby facilitating assembly with other tool component in order to produce specialized mission support tools. The presence of specialized tools is critical to quickly evolving cyber protection.

c. The deployment of the USCYBERCOM Capability Repository. The USCYBERCOM Capability Repository assists with the rapid development of cyber modules and cyber systems by documenting the link between existing IT assets and IT capabilities that can be combined to deliver cyber modules and cyber systems. This critical deployment must be completed by the third quarter of FY 2016.

d. The delivery of an Open Source Tool Kit, due by the end of November 2015, which has distinct visibility within DoD. This Open Source Tool Kit will identify new, emerging, and undervalued open source solutions to cyber security and will provide a starting point for DoD organizations when evaluating open source solutions for deployment.

e. Conduct proofs of concepts and prototype development. Proofs of concepts are used to test aspects of an intended design without exact simulation. Working prototypes will simulate the final functionality of an intended design.

f. Conduct vulnerability analysis and survey network services and/or applications to pair with security vulnerabilities.

g. Conduct research on cyber capabilities in association with vulnerabilities to determine weaknesses and methods of exploitation.

h. Provide advanced technical consulting as related to development efforts.

i. Proactively engage military planners, operators, testers, and other developers to learn about mission objectives and cyber capabilities.

j. Perform scheduling and resourcing of developers and review associated documentation as required.

k. Perform computer network exploitation development: Embedded reverse engineering (RE), vulnerability research (VR), and application development for software and embedded systems with a focus on Cyber Operations, CAN and Computer Network Exploitation (CNE) activities.

l. Evaluate the quality of proposed and existing software systems and solutions that support various cyber software activities and are planned to be integrated into various networks and architectures.
m. Conceive, propose, design, and develop software in support RDT&E work to develop cyber tools and techniques to mitigate identified vulnerabilities.
n. Perform needs and risk analysis of software packages (developmental Government-off-the-Shelf (GOTS) and Commercial-off-the-Shelf items (COTS)) relative to mission requirements.
o. Develop, update, and evaluate software engineering standards, specifications, handbooks, or manuals in relation to the development and testing of cyber capabilities.
p. Document verification and validation of solution sets and protocols, and provide technical assistance to user organizations with all aspects of software acquisition.
q. Develop life cycle models and customize software analytical tools, models, decision aids, screening methods and techniques used to evaluate and support the authenticity and continuity of DoD, national, commercial, and international information systems.
r. Develop specialized software/firmware modules to run on embedded hardware that communicate across native communications channels and implement specialized functions on embedded systems.
s. Disassemble and analyze software and embedded firmware.
t. Mentor other staff to improve RE skills.
u. Collaborate with Cyber Innovation Unit staff working multifunctional programs integrating hardware and software RE tasks.
v. Assemble and establish the software development environment.
w. Recommend software tools and applications.
x. Perform data transfer.
y. Conduct systems administration.
z. Review and potentially enhance legacy code.
aa. Draft documentation.
bb. Conduct developmental testing.
cc. Perform peer software and documentation reviews.

C.5.5 TASK 5 – PROVIDE CAPABILITY AND RESOURCE INTEGRATION SUPPORT (J8)

The contractor shall support the Government task lead in advocating for the Warfighter within DoD's three decision support systems: the Joint Capabilities Integration and Development System (JCIDS), the Defense Acquisition System (DAS), and the Planning, Programming, Budgeting, and Execution (PPBE) system. Together, the systems provide an integrated approach to strategic planning, capabilities needs assessment, systems acquisition, and program and budget development. DoD uses the DAS to manage the acquisition of weapon systems and major automated information systems (MAIS). Although based on centralized policies and principles, the system allows for de-centralized and streamlined acquisition. The system is flexible and encourages innovation, while maintaining strict discipline and accountability. The Joint Chiefs of

Staff developed JCIDS to assess and resolve gaps in military joint warfighting capabilities. The PPBE Process is DoD's resource determination process. DoD uses PPBE to craft plans and programs that satisfy National Security Strategy demands within resource constraints, providing the Warfighter the capabilities necessary to accomplish assigned missions.

The contractor shall support J8 developing, assessing, validating, prioritizing, documenting and maintaining requirements and associated requirements products.

The Government anticipates that the support shall include, but is not limited to the following:

a. Provide analysis, subject matter expertise and administrative technical support for the implementation of USCYBERCOM Requirements Management process for capturing, evaluating and prioritizing resource and capability requirements across the USCYBERCOM to generate a balanced program that optimizes activities and expenditures to support the mission.
b. Work collaboratively with stakeholders to identify, document and validate requirements. This requires active engagement with technical and functional SMEs for the purpose of substantively affecting the decision-making process. The nature of the requirements is highly technical in nature and requires subject matter expertise in current and emerging cyberspace concepts and applications, and evaluation of their relative contributions to the mission and key program objectives.
c. Provide subject matter expertise to conduct, assist, organize and facilitate the creation of **Joint Capabilities Integration and Development System Documentation (Section F, Deliverable 15)** concerning cyberspace initiatives.
d. Assist in the operational and technical analysis required in defining and drafting requirements documentation, which defines the capability gap; summarizes the results of Doctrine, Organization, Training, Materiel, Leadership and education, Personnel and Facilities (DOTMLPF) analysis; and describes why non-materiel changes alone may have been judged inadequate in fully providing the capability. This documentation is vital to initiating research, experimentation and new capability efforts to support the warfighter mission.
e. Assist the Government in conducting annual capability gap validation/re-validation of existing gaps before every program build/project execution to identify capability needs or gaps throughout the year in response to emerging threats, changing external guidance, and realignment of mission priorities.
f. Contribute to efforts to create and establish automated tools supporting the USCYBERCOM’s Requirements Management process including the following:
    1. Participate and provide subject matter expertise in efforts to establish performance specifications for automated tools supporting the Requirements Management process.
    2. Provide Test and Evaluation support of the requirements management software and processes.
    3. Participate in assessment of alternative design concepts and testing of prototypes.
    4. Make use of these tools to generate a variety of recurring and unique reports.

5. Make use of lessons learned to recommend refinements in supporting tools and, as such recommendations are approved, collaborate with J6 to design/develop, validate and implement them across USCYBERCOM.

g. Provide subject matter expertise to conduct analysis of test data, modeling or simulation efforts, Manpower and Personnel Integration (MANPRINT), evaluations of embedded software, contractor technical services, and methodology studies to assist, organize and facilitate the cyberspace program community in Capabilities Base Assessments (CBAs). The objective of CBAs is to validate perceived capability gaps by showing relationships to the DoD cyberspace mission, defining/documenting proposed capabilities and associated operational characteristics and attributes, showing how these proposed capabilities will address capability gaps and associated operational risks of inaction, identifying and assessing non-materiel solutions, and making recommendation on what type of solution shall be pursued (and funded).

C.5.6 TASK 6 – PROVIDE PROGRAM AND TECHNICAL SUPPORT (J6 AND J8)

The contractor shall provide program and technical support to the J6 and J8 Directorates.

C.5.6.1 SUBTASK 1 – PROVIDE PROGRAM SUPPORT (J6 AND J8)

The contractor shall support USCYBERCOM'S J6 and J8 Directorates in providing program oversight and systems engineering of cyberspace, and cyberspace-related, developmental activities across the DoD community research and development portfolios, of which USCYBERCOM is invested. The contractor shall provide support to include, but not limited to, the following:

a. Perform outreach activities to Cyber Operations capability developers and providers to understand new and emerging technology.
b. Provide systems engineering based recommendations (per 2009 DoD Systems Engineering Process Model) leading to the design and realization of Cyber Operations technologies into capabilities based on USCYBERCOM prioritized operational requirements.
c. Evaluate and recommend strategies, as required, to synchronize DoD community research and development in support of prioritized operational requirements.
d. Provide recommendations, as required, for the transition of cyberspace prototype solutions to acquisition centers, or operational units, for further engineering, manufacturing and development, operations, or sustainment.
e. Assist USCYBERCOM in general engineering support such as addressing command actions, developing plans and responses, articulating strategies for future directions, and formulating the processes and frameworks necessary to support the DoD community capability development, followed by capability transition.

C.5.6.2 SUBTASK 2 – PROVIDE TECHNICAL SUPPORT (J6)

The contractor shall contribute to joint architectural/systems engineering analyses to validate that proposed C4 designs can be fully integrated with existing projected and target information systems (IS) enterprise architectures, and that they facilitate effective communications and authorized exchange of information. The contractor shall contribute to cyberspace operations

community-level IS enterprise architecture business processes, including governance boards and working groups. The contractor shall support development of a cyberspace operations community-level milestone review process, and support its implementation to ensure collaboration among representatives of cyberspace operations partners in the identification and coordination of new and proposed C4 investments and initiatives,

The contractor shall provide support to include, but not limited to, the following:

a. Synthesize enterprise system and service requirements based on broad customer needs.
b. Review the specification and design of enterprise system and service architectures in a distributed, net-centric environment.
a. Leverage DoD policies, architectural frameworks, and commercial best practices for the design and development of Service Oriented Architectures (SOAs) that satisfy enterprise scale requirements.
b. Define the CONOPS and TTPs for the system's use within the enterprise.
c. Provide subject matter expertise on new enterprise architecture solutions including leading edge technologies such as grid computing, cloud computing, and SOA.
d. Provide subject matter expertise on commercial technologies and other Government initiatives to identify opportunities for technology reuse or transition.
e. Perform technical planning, system integration, verification and validation, cost and risk, and supportability and effectiveness analyses for total systems.
f. Perform duties such as site surveys, system evaluation, system analysis, architecture, and infrastructure assessment.
g. Ensure the logical and systematic conversion of customer or product requirements into total systems solutions that acknowledge technical, schedule, and cost constraints.
h. Support analytical modeling to describe utilization and performance at multiple levels of granularity.
i. Support resource chargeback rate-setting activities.
j. Analyze the impact of new technologies on processor and peripheral utilization and performance.
k. Support workload sizing for new and existing applications.
l. Support the implementation of hardware and software upgrades.
m. Support the construction of capacity plans.
n. Utilize systems that analyze and report levels of utilization and performance.
o. Oversee storage of capacity and performance data.
p. Support disaster recovery sizing activities.
q. Support the measurement and reporting of service level objectives.

The contractor shall conduct reviews and provide feedback of technical materials consisting of, but not limited to, technical documentation and reports, cyber policy and procedures, and planning materials. These documents will be identified and provided by the Government SMEs. The contractor shall assist with data collection and analysis for USCYBERCOM cyber presentations, speeches, briefings, and maintain monthly quarterly and annual metrics on leading security indicators, as required. The contractor shall review cyber-related input from various

organizations, assembling the information into a consolidated package, and submit it for inclusion into various cyber recurring and by demand reports (e.g., Director's/Commander's Weekly Activity Report (WAR) and quarterly and annual NetOps reports). The contractor shall analyze security details of systems, assist with developing and publishing security processes and produce official records from formal IA meetings of every category. The contractor shall use current doctrine, publications, and coordination methods with other responsible organizations involved with USSTRATCOM as a basis for planning and support.

C.5.7 TASK 7 – PROVIDE TECHNICAL ASSISTANCE (J6 AND J9)

The contractor shall support the network and lab environments that facilitate the TA evaluations and development of new advanced cyber technologies and emerging cyber capabilities. In addition, the contractor shall provide subject matter expertise in web development and web application functionalities.

C.5.7.1 SUBTASK 1 – PROVIDE NETWORK ENGINEERING SUPPORT (J9)

The contractor shall support USCYBERCOM's J9 Directorate by providing network engineering support to the infrastructures required to support the TA evaluations test environments (Section C.5.2.2, Conduct Technical Assurance Evaluations and Operational Assessments) and the experiment research environments (Section C.5.4, Research, Develop, Analyze, and Test Cyber Related Capabilities). Each network environment supported will be specific to the nature of the requirement and will vary in size and complexity.

The contractor shall provide support to include, but not limited to, the following:

a. Determine user requirements and design specifications for networks.
b. Monitor closed networks, each with a specific support the network environment, to ensure network availability to system users. Perform necessary maintenance to support the closed network availability. The closed networks must maintain a 95 percent availability.
c. Plan, schedule, and conduct the installation of new or modified hardware and associated operating systems, and software applications. Updates to software operating systems and applications are anticipated weekly at a minimum, hardware replacements are as needed but anticipated annually.
d. Design and conduct tests and evaluations of networks. The Government anticipates that existing COTS and GOTS tools will be utilized to satisfy the network tests and evaluations.
e. Analyze and organize the corresponding hardware and software combined solutions through network modeling and planning.
f. Perform system-level design and configuration of products including determination of hardware, operating system, and other platform specifications.
g. Evaluate new network technologies and provide **Technology Recommendations (Section F, Deliverable 16)** to the Government regarding integration of these technologies into the existing network.
h. Plan and provide new **Network Configuration and Integration Plans (Section F, Deliverable 17)** for existing networks to maintain optimal performance.

i. Provide subject matter expertise to achieve joint full spectrum network interoperability and integration.
j. Support system integration by writing reports, attending planning sessions, and conducting analysis of current/future network conditions.

The contractor shall provide **Service Engineering and Technical Reports (Section F, Deliverable 18)** that document the results of studies and analyses as required by the Government. Examples of Service Engineering and Technical Reports include:

a. Commander-Level Documents
b. Training Plans
c. Implementation Plans
d. Tactics and Techniques Documents
e. Procedures, Processes, and Schedules.

C.5.7.2 SUBTASK 2 – PROVIDE LAB MANAGEMENT SUPPORT (J9)

The contractor shall support J9 by managing the operation and sustainment of all equipment, software, hardware, within the testing laboratories and support the full operation of the testing laboratories that facilitate activities detailed in Section C.5.2.2, Conduct Technical Assurance Evaluations and Operational Assessments, and in Section C.5.4, Research, Develop, Analyze, and Test Cyber Related Capabilities. The contractor shall manage test beds, hardware, software, software repositories, and lab documentation. The contractor shall evaluate and recommend hardware/software for the labs and assist with resolving discrepancies in USCYBERCOM property accountability.

The contractor shall support the continued development of the cyber immersion training environment, which shall establish a centrally-managed training environment to simulate real cyber-attack scenarios that shall support the CMF.

C.5.7.3 SUBTASK 3 – PROVIDE WEB DEVELOPMENT SUPPORT (J6)

The contractor shall support existing web development and web-based initiative functions that are executed in real time to meet mission requirements. The contractor shall perform related test and evaluation, TTP development, and user training. The contractor shall support web application development that occurs in the following tools or languages: SharePoint, HTML, CSS, XML, .NET, ASP, C#, SQL, Java Script and AJAX.

C.5.8 TASK 8 – PROVIDE INFORMATION ASSURANCE (IA), CONFIGURATION MANAGEMENT (CM) AND TECHNICAL WRITING SUPPORT (J6, J8, AND J9)

The contractor shall provide IA, CM, and technical writing support to USCYBERCOM's J6, J8, and J9 Directorates.

C.5.8.1 SUBTASK 1 – PROVIDE IA SUPPORT (J6, J8, AND J9)

USCYBERCOM is currently refining and tailoring the DoD 8570.01-M, *Information Assurance Workforce Improvement Program*, into actionable IA guidance that can be utilized to assist in USCYBERCOM mission. The contractor shall support IA activities such as developing Systems

Security Plans (SSP's), conducting vulnerability scans, and providing technical expertise in IA. The contractor shall provide support to include, but not limited to the following:

a. Provide training for the USCYBERCOM Cybersecurity Workforce Improvement Program (WIP, also known as IAWIP) and USCYBERCOM IA Program to ensure an informed, alert, and security conscious workforce. This includes adjustments to current training materials to account for finalized guidance.
b. Develop tracking tools for mandated DoD Cybersecurity WIP certification status reports to include, at a minimum, the following information:
    1. Fully compliant and certified personnel.
    2. Personnel required to take training for certification.
    3. Noncompliant personnel required to take immediate remedial action.
c. Develop websites and/or databases to manage data for USCYBERCOM IA and IAWIP programs.
d. Develop consolidated metrics data for periodic status reports, and provide inputs to the Federal Information Security Management Act (FISMA) report and Information Assurance Manager (IAM).

The contractor shall provide vulnerability scanning, auditing support and develop mitigation resolution, as necessary, to ensure cybersecurity compliance with DoD/NSA IAVA/STIG and USCYBERCOM 5200-08 requirements and provide status reports to the USCYBERCOM Cybersecurity Managers and to System Administrators.

C.5.8.2 SUBTASK 2 - PROVIDE CM SUPPORT (J6, J8, AND J9)

The contractor shall provide CM support to include, but not limited to the following:

a. Log capability submissions.
b. Disseminate reports.
c. Prepare evaluation certificates.
d. Archive all distributed reports evaluation materials.
e. Maintain records of all evaluation activities.
f. Generate statistics tailored to Government management requirements.

The contractor shall log all lab hardware, software, and documentation into a database and successfully retrieve materials as needed. The contractor shall also inventory all database items on a periodic basis, search for missing items, and prepare paperwork to excess unwanted items. The contractor shall assist with resolving discrepancies in USCYBERCOM property accountability.

C.5.8.3 SUBTASK 3 – PERFORM TECHNICAL WRITING (J6, J8, AND J9)

The contractor shall review, edit, and format technical reports to improve the flow and grammar of the technical content. The contractor shall work with the technical staff to resolve inconsistencies and develop **Document Templates (Section F, Deliverable 19)** and record **Meeting Minutes (Section F, Deliverable 20).**